다중코어 환경에서의 멀티캐스트 보안에 관한 연구

이 준 석**

A Study on the Multicast Security System in Multiple Core Environment

Jun-Seok Lee

ABSTRACT

Multicast is a network technology for the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the multiple destinations split. This thesis designed a group certificate that can authenticate group information safety between cores based on CBT, proposed a multicast security system that can control some security key.

keyword 멀티캐스트, 멀티캐스트 보안, 다중코어

Ⅰ. 서 론

멀티캐스트(multicast)는 인터넷상에서 전자메일과 같은 데이터(data), 영상, 음성데이터 등을 특정 사용자 그룹인 둘 이상의 다른 수신자들에게 동시에 전송하는 방식이다. 이러한 멀티캐스트는 특정한 한 사람의 수신자에게만 데이터 패킷을 전송하는 방식인 유니캐스트(unicast)와 대응하는 개념이다.

유니캐스트 방식에서는 받는 사람의 수만큼 데이터 패킷(data packet)을 반복해서 보내야 하기 때문에 통신망의 효율을 저하시키고, 보내는 사람의 전송 부담도 크다. 그러나 다자간 화상회의와 같은 대화형 인터넷 기능에서는 음성 및 화상 데이터의 실시간 전송이 필요하므로 동시에 여러 명이 데이터를 주고받는 멀티캐스트 방식이 필수적이며, 이러한 멀티캐스트 전송방식은 데이터 중복전송으로 인한 네트워크 자원낭비를 막고, 그

* 본 연구는 2008년도 동남보건대학 연구비 지원에 의하여 수행된 것임.
** 동남보건대학 경영학과 부교수.

정보를 필요로 하지 않는 곳에는 부담을 주지 않으면서 실시간 공동작업을 효율적으로 보장하는 전송기법이다. 멀티캐스트 전송이 일반적인 유니캐스트 인터넷 응용 분야와 다른 점은 전송 패킷에 있다. TCP/IP 상의 인터넷 응용 프로그램은 데이터의 송신자가 이를 수신할 수신자의 인터넷 주소를 전송 패킷의 헤더에 표시해 패킷을 전송한다. 그러나 멀티캐스트 전송을 위해서는 헤더에 수신자의 주소 대신 수신자들이 참여하고 있는 그룹 주소를 표시하여 패킷을 전송한다. 멀티캐스트 전송을 위한 그룹 주소는 D-class IP 주소 (224.0.0.0~239.255.255.255)로 개개의 인터넷 호스트를 나타내는 A, B, C-class IP 주소와는 달리 실제의 호스트를 나타내는 주소가 아니며, 그룹 주소를 갖는 멀티캐스트 패킷을 전송받은 수신자는 자신이 패킷의 그룹에 속해있는 가를 판단해 패킷의 수용여부를 결정하게 된다. 그러나 현재 인터넷상의 라우터들이 대부분 유니캐스트만을 지원하기 때문에 멀티캐스트 패킷을 전송하기 위하여서는 멀티캐스트 라우터 사이에 터널링(tunneling)이라는 개념을 사용하여 캡슐화(encapsulation)된 패킷을 전송한다. 즉 멀티캐스트 주소를 가진 데이터 패킷 헤더 앞에 멀티캐스트 라우터간에 설정된 터널의 양 끝단의 IP 주소를 덧붙여 라우팅(routing)을 함으로써 멀티캐스트를 지원하지 않는 일반 라우터들을 거칠 때 기존의 유니캐스트 패킷과 같은 방법으로 라우팅되어 최종적으로 터널의 종착지로 전송될 수 있게 하는 것이다.

이호영(2007)은 이러한 멀티캐스트 방식의 경우 모든 정보가 디지털로 전송되고 통신망 자체가 개방성을 갖기 때문에 정보 자원에 대한 위협이 심각하게 증가하고 있으므로, 이에 대한 보안의 위협으로부터는 안전한 멀티캐스트 통신을 위한 보안 시스템에 대한 연구가 필요하다고 하였다.

원격 화상. 음성 회의, 다중 사용자 게임, 유료 영상 서비스, 주식 시세 배포, 소프트웨어 다운로드 등 멀티캐스팅 서비스들은 점차 다양해지고 사용자의 폭도 점차 넓어지고 있다. 그러나 서비스가 발전하고 사용도가 높아지게 되면 그에 비례하여 해커들의 공격 대상으로 주목 받게 되고 정보의 누출 가능성도 높아진다. 따라서 멀티캐스팅 서비스 활용과 동시에 그에 대한 보안 연구도 함께 이루어져야 한다.

그러나, 현재까지는 멀티캐스트 보안 서비스나 보안구조 그리고 안전한 보안 시스템에 대한 연구가 많이 진행되지 않았으며, 단일 코어만을 가진 단일 통신 환경에서의 확장성에 대한 문제점을 보완하면서 이러한 보안 위협을 해결하기 위한 연구만이 진행되고 있다.

이러한 필요성에 따라 다중 코어(multi core)를 갖는 통신 환경에서 사용자 데이터를 안전하게 전송할 수 있도록 CBT(Core Based Tree) 멀티캐스트 라우팅 프로토콜(multicast routing protocol)을 기반으로 코어간에 그룹 정보를 안전하게 인증할 수 있는 멀티캐스트 그룹 인증서를 설계하여, 보안키를 원활하게 분배하고 제어할 수 있는 멀티캐스트 보안 시스템을 설계하고, 멀티캐스트 통신을 위해서 연구가 진행되고 있는 멀티캐스트 라우팅 프로토콜과 현재 사용되고 있는 멀티캐스트 라우팅 프로토콜 중에서 보

다 효율적인 보안 체계를 설계할 수 있고 확장성에 있어서도 루트(root)에게 모든 트래픽(traffic)이 집중되지 않고 중간 라우터에서 인증과 보안키를 교환 할 수 있는, 분산환경에 적합한 공유 트리(shared tre)를 기반으로 하는 CBT를 이용하여 멀티캐스트 보안 시스템을 설계하였다.

Ⅱ. 멀티캐스트 보안 서비스

멀티캐스트 보안 구조 설계는 네트워크 프로토콜(network protocol)과 네트워크 사이트(network site), 그리고 네트워크 사이트와 호스트(host)간의 관계에 많은 제어 기능을 배치하도록 고려해야 한다.

바람직한 보안 설계는 기존의 네트워크 프로토콜과 호환되고 광역 인터넷의 범위로 확장할 수 있으며 투명성을 가져야한다. 또한, 보안 구조는 상위 레벨 응용에 의해 요구되는 것과 같이, 다양한 세션 제어의 정책을 지원하는데 유연해야 한다. 이들 특징들은 인터넷과 같은 기존의 환경에 믿을 수 있는 멀티캐스트를 쉽게 통합시킬 수 있게 한다.

1. 인증

인증은 기존의 세션에 가입하도록 요구하는 멀티캐스트 주소와 스크린 호스트(screen host)의 등록을 제어하기 위한 신뢰받는 멀티캐스트에서 필수적인 메커니즘이다. 때때로, 가입을 요구하는 참가자와 기존의 세션 멤버(session member)는 상호 인증을 요구한다. 경우에 따라, 한 참가자는 다른 참가자에게 인증을 위임하기도 한다.

인증을 요구하기 위해서는, 비록 인증 수행이 새로운 참가자가 그룹을 가입함으로서 가입 절차가 증가하더라도, 크기 n의 그룹에 대한 인증 프로토콜의 O(n2)에 수행되기를 요구한다. 그러나 이것은 인증 절차에 상당한 분담을 가지게 한다. 그래서 좀 더 효과적인 방법은 새로운 멤버를 확실히 인증하기 위해서 다른 그룹 멤버에 의해 신뢰받는 그룹 리더를 선택하는 것이다. 이 경우에서, 그룹 리더는 사실상 그룹 멤버쉽 정책을 제어한다. 자연적인 그룹 리더 선택은 세션 초기자를 그룹 리더로 하는 것이다. 세션 초기자가 세션을 등록할 때, 이것은 그룹 리더가 되고 입회 정책을 명시한다. 만약 그룹 리더가 고장나고 임기 만료되면, 새로운 리더가 세션 정책에 의해, 안전한 프로토콜을 통해서 선택되어야 한다.

멤버가 자진해서 또는 다른 이유로 세션을 탈퇴할 때, 멤버는 정확히 종료하여야 한다. 그렇게 하지 않으면, 이 멤버는 그룹에 가입하지 않고 나중에 도청을 할 수 있다. 또

한 탈퇴한 멤버의 잔류 정보가 잠재적인 공격자에 의해 부당하게 이용될 수 있다.

2. 안전한 세션

그룹 지향 분배 시스템에서는 안전한 세션을 위해서 다음과 같은 몇 가지 사항을 고려해야한다.

1) 세션 멤버쉽 정책

세션은 다양한 형태의 멤버쉽 정책을 가지고 다양한 목적을 위해서 설정될 수 있다. 멀티캐스트 관리를 위해서 몇 가지 일반적인 정책이 존재한다. 첫 번째는, 참가자가 허가 없이 자유롭게 참가할 수 있는 뉴스그룹과 같은 개방 세션이고, 두 번째는 도시의 특정 건물처럼, 참가자가 자유롭게 참가할 수 있는 개방된 세션이지만 참가자는 안전 검사를 통과해야 하고, 세션 중개자가 있어야 하는 반-개방 세션이다. 마지막으로, 의회의원들만이 참가할 수 있는 의회회의와 같은 제한된 세션이다.

2) 등록과 등록 취소

호스트 또는 사용자가 멀티캐스팅 세션(multicasting session)을 확립하기 위해서 네트워크 주소를 요구할 때, 멀티캐스팅 관리 센터(MMC: Multicasting Management Center)는 요청자의 식별을 검증하고 세션을 등록할 수 있는 자가 요구하는 세션 정책을 검사한다. 요청자는 세션이 정확하게 등록되도록 MMC의 식별을 검증하기를 바랄 것이다. 멤버쉽 정책, 사용자 증명서, 등록된 세션의 기록 같은 정보는 접근 제어 목록형태의 MMC에 저장된다.

MMC에서 세션이 도착하는 것을 등록 취소하도록 요청할 때는 요청자를 인증해야 하고 만약 이러한 요구에 대해 인증이 되면 종료한다. 일반적으로 세션 리더 또는 이것의 대리인만이 세션을 등록 해제할 수 있다. 만약 멀티캐스트 세션이 바람직하지 못하면 세션은 종료된다.

3) 세션 가입과 탈퇴

세션 멤버 사이의 통신은 공개적으로 또는 개인적으로 할 수 있다. 이러한 사항은 등록 시간에 명시하고 나중에 변경할 수도 있다. 이것은 개별적인 멤버의 재량에 따라 속성을 가짐으로서, 몇 몇 통신은 공개적인 통신을 하면서 동시에 개인적인 통신을 할 수 있다. 대부분의 네트워크는 네트워크 트래픽 도청에 의해 공개되기 때문에, 멀티캐스트

에서 개인적인 세션을 위해서는 충분한 프라이버시 준비가 요구된다. 가입과 탈퇴가 요청될 때, 인증된 자만이 메시지를 정확히 복호화할 수 있도록 보증하기 위해서 메시지 내용을 암호화 필요가 있다.

4) 안전한 세션 통신

안전한 세션 통신을 위해서는 다음과 같은 방법이 사용된다. 모든 세션 멤버에 의해서 공유된 공통 암호화키의 분배를 사용하고 이 그룹 키를 이용해 브로드캐스트 메시지를 암호화하는 것이다. 이 접근을 이용하여, 초기 키 분배는 세션이 등록될 때 발생해야 한다. 이 키는 세션 리더 또는 인증 서버에 의해 선택될 수 있다. 이 키는 세션 리더에 의해 유지되거나 세션이 등록되는 MMC에 저장된다. 누군가가 세션에 가입될 때, 그룹 리더 또는 MMC는 세션 정책을 검사한다. 새로운 멤버가 세션으로 받아들여질 때, 이것은 MMC 또는 그룹 리더로부터 그룹 키를 수신한다. 그룹 리더가 고장나면, 기존에 많이 알려진 선택 프로토콜을 이용하여 새로운 리더가 선택된다.

5) 안전하고 효과적인 브로드캐스트

멤버는 새로운 멤버쉽을 위해서 메시지 당 새로운 암호화키를 선택할 수 있다. 그러므로 탈퇴하는 멤버에 의한 키 누출의 위험은 상당히 감소되고 새로운 그룹 키를 할당할 필요가 없다.

각 멤버는 공개키와 개인키를 지원하는 RSA 암호화 시스템을 사용할 수 있다. 메시지를 브로드캐스트(broadcast)하기 위해서, 멤버는 DES에서 사용하기 위해 랜덤(random)하게 암호화 키를 선택하고 메시지를 암호화한다. 멤버는 개인키를 이용하여, 재전송 공격을 방어하도록 타임스탬프, DES 키, 무결성 검사합을 제공하기 위해 원 메시지의 단방향 해쉬 함수(hash function)를 서명한다. 그리고 멤버는 서로 멤버의 공개키를 이용하여 이 서명을 암호화한다. 마지막으로, 암호화된 서명과 암호화된 메시지를 n-1번 브로드캐스트(또는 멀티캐스트)한다.

세션 멤버쉽 변경을 통고할 때, 멤버는 탈퇴자를 포함한 세션의 외부에 있는 사람이 판독할 수 없도록, 간단히 그들의 로컬 멤버쉽 목록을 갱신하고 차후의 멀티캐스트를 위해서 새로운 DES 키를 선택한다.

6) 암호화 모드

멀티캐스트는 응용 환경에 따라, 다중 암호화 모드들 사이에서와 블록 암호화와 스트림(stream) 암호를 이용하는 사이에서 요구될 수 있다. 예를 들어, ECB 모드는 메시지의 개별적인 블록에서 랜덤 접근을 허가한다. 또한 스트림의 사전연산이 가능한 스트림 암호화는 일반적으로 블록 암호보다 빠르지만, 데이터 손실이 발생할 때 재 동기화의 비용

때문에, 높은 신뢰를 가지는 환경에서 더 적당하다.

그리고 스트림의 일부분만 암호화하는 경우를 고려해야 한다. 전체 스트림을 암호화하는 것은 효율성 때문이다. 반면에, 부분 암호화는 스트림의 암호화 시간과 복호화 시간을 줄여준다. 따라서 여분의 시간을 화상의 해상도나 오디오 음향 처리에 사용할 수 있다. 예를 들어, 그림의 배경은 공개적이지만 가운데의 사람 이미지는 특별한 처리를 요구하는 경우에 유용하다.

7) 세션 통지(session advertising)

많은 서비스는 통지되어질 필요가 있다. 등록된 세션은 게시판 서비스와 같은 것에 의해서 고유의 증명서와 신원 정보를 제공하여야 한다. 그래서 이들은 통지의 인증을 점증할 수가 있다. 경우에 따라서는 서비스 정보의 통지를 제한할 필요도 있다, 이런 경우에는 게시판을 안전한 다중 레벨(multi-level) 형태로 만들어야 한다.

3. 트리 접근의 제어

각 네트워크 교환은 하나 또는 그 이상의 인증 서버에 소유되는 개인키와 대응하는 공개키를 유지한다. 새로운 연결이나 기존 연결의 수정을 위한 요청을 초기화하기 전에, 호스트는 먼저 인증 서버에 요청 메시지를 전송한다. 호스트를 인증한 후에, 서버는 서명이 첨부된 메시지를 반환 전송한다. 메시지는 네트워크 경로를 따라서 전송되고 경로의 모든 교환은 서명에 대하여 지역 서버의 공개키를 이용하여 검사한다. 또한, 트래픽에 삽입되기를 원하는 노드(node)는 서버로부터 서명을 먼저 획득해야 한다. 네트워크 노드는 이러한 서명 없이 발신지로부터 트래픽을 받아들일 수 없다.

수신자의 인증은 상대적으로 드물게 수행됨으로 교환에서 큰 처리 부담을 가지지 않는다. 반면에, 비 인가된 발신지를 막기 위해서, 패킷(packet)에 서명을 전송하는 것은 교환에서 부담을 가중시킨다. 특히, 화상과 같은 스트림 트래픽에서 더욱 심각하다. 스트림 트래픽 교환을 위해서는 단지 패킷의 일부분이 서명을 운송하고 교환은 이들 서명을 운송하지 않는 패킷의 전송을 위해서 서명을 캐쉬 해야 한다. 캐쉬(cache)는 가끔 갱신되어야 한다.

정크 패킷을 이용하여 멀티캐스트 주소를 폴르딩하거나 가짜 멀티캐스트 세션을 설정함으로서 악의 있는 참가자는 네트워크 자원을 공격할 수 있다. 따라서 가능하면 멀티캐스트 발신지의 근처에서 이러한 정크 패킷을 식별하여 막도록 하여야 한다. 그렇지 않고 목적지에서 정크 패킷을 식별하면 그것이 목적지에 도착할 때까지 귀중한 네트워크 자원이 소비되어진다.

4. 확장성과 최적안

사용자 또는 호스트 인증을 위해서 할당되는 초기의 암호화키의 과제는 안전한 멀티캐스트에 참가하고자 하는 사용자 또는 호스트의 숫자가 산술적으로 커진다는 것이다. 세션을 확립하기 위해서, 세션 멤버쉽을 교환하기 위한 메시지의 숫자는 세션 크기에 따라 커진다. 안전한 브로드캐스트 알고리즘은 메시지마다 동적인 암호화 키 변경을 허가함으로서 그룹 멤버쉽 변경에서 새로운 그룹 키를 요구하는 것을 제거할 수 있다. 그러나 가입과 탈퇴가 더 이상이 발생하지 않는 상태가 되면 그룹 멤버쉽이 적당히 안정되어 메시지마다 새로운 암호화 키를 사용하는 암호화 방식보다 그룹 키를 사용하는 것이 좀 더 효과적이다.

때때로, 세션의 멤버는 많은 양의 그룹을 형성한다. 예를 들어, 원격회의 응용에서, 비록 모든 멤버들의 음성이 모든 목적지에 브로드캐스트 되더라도, 멤버는 단지 자신의 근처에 있는 멤버에게만 물리적 위치 정보(자신의 좌표)를 브로드캐스트 하기를 원할 것이다. 이 같은 그룹을 구성하기 위해서, 데이터 암호화키는 메시지 당 암호화키를 동적으로 선택할 수 있기 때문에, 멤버는 다수의 그룹키를 저장할 필요가 없다. 물론 멤버는 멤버쉽 변경이 발생할 때까지 데이터 암호화키를 저장하고, 서명된 메시지 헤더를 대응시키고, 그들을 재 사용함으로서 최적화될 수 있다.

5. 다중 레벨의 안전한 멀티캐스트

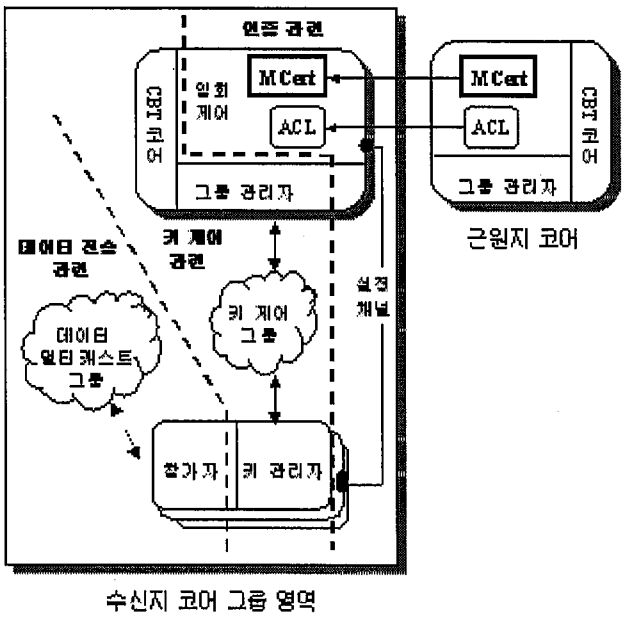
그룹들과 멤버들은 서로 다른 레벨로 분류될 수 있다. 그리고 참가자는 자기 자신보다 높은 보안 레벨을 가진 그룹의 멤버가 될 수 없다. 또한 레벨은 암호화키를 할당받고 레벨이 좀 더 높은 곳의 키에 대해서는 접근할 수 없다. 암호화를 위해서, 키의 레벨은 평문의 레벨보다 동등하거나 높아야한다. 암호문의 레벨은 이때의 키의 레벨이다. 이러한 할당은 가상 네트워크로 멀티캐스트 네트워크를 효과적으로 분리한다.

다중 레벨 보안은 높은 레벨 그룹 멤버가 낮은 레벨 정보를 접속할 수 있음을 요구할 것이다. 이것을 확립하는 하나의 방법은 낮은 레벨 그룹 멤버가 멀티캐스트 메시지를 높은 레벨의 그룹에게 전송할 수 있도록 하는 것이다. 그런데, 송신자가 일반적으로 적당한 높은 레벨의 암호화키를 가질 수 없기 때문에, 높은 레벨 멤버가 낮은 레벨 키를 사용할 수 있도록 하거나 낮은 레벨 키를 이용해서 전입 메시지를 복호화하고, 메시지를 중계하기 전에 높은 레벨 키를 이용해서 메시지를 재 암호화하는 게이트웨이를 다중 레벨 네트워크 구성요소에 포함시키는 것이다.

Ⅲ. 멀티캐스트 보안시스템 설계

<그림 1>은 제안된 키 분배 프로토콜을 위한 송신자와 수신자가 확실하게 구별되지 않는 다중 그룹 통신에서의 멀티캐스트 보안 모델이다. 제안된 보안 구조의 구성요소는 3개의 그룹으로 구성된다. 하나는 그룹 통신에 참가하고자하는 각 참가자가 코어로부터 인증을 받는 인증 관련 부분이고 두 번째는 참가자가 데이터 전송을 위해 코어 기반 트리에 가입하는데 관련되는 키 제어 관련 부분, 그리고 세 번째는 안전한 멀티캐스트 데이터를 전송하는데 관련된 데이터 전송 관련 부분으로 나누어진다.

1. 데이터 전송 관련



[그림 1] 다중통신 환경에서의 멀티캐스트 보안 시스템

1) 참가자(participant)

멀티캐스트 통신을 하는 주체로서, 로컬 키 관리자가 생성한 트래픽 암호화 키(TEK: Traffic Encryption Key)와 그룹 관리자로부터 주어진 키 암호화 키(KEK: Key Encryption

Key)를 이용하여 전송하고자하는 패킷을 암호화하여 데이터 멀티캐스트 그룹으로 데이터를 전송하고 전송되어온 메시지를 로컬 키 관리자로부터 주어진 키를 이용하여 복호화 한다.

2) 데이터 멀티케스트 그룹(data multicast group)

멀티캐스트, 브로드캐스트, 또는 유니캐스트 채널은 적어도 의도된 수신자에게 송신자로부터 안전한 패킷을 전달한다. 이것은 대부분의 응용 데이터를 전송하는데 사용된다.

2. 키 제어 관련

1) 그룹 관리자(gruop manager)

참가자로부터 가입과 탈퇴 요청을 수신하고 허가하고 처리한다. 그리고 필수적인 키 교환을 수행하기 위해 키 관리자에게 메시지를 송신한다.

2) 키 제어 그룹(key control group)

멀티캐스트, 브로드캐스트 또는 유니캐스트 채널은 그룹 관리자로부터 의도된 수신자에게 패킷을 전달한다. 트래픽은 참가자의 키 관리자에게 분배되는 새로운 키잉 재료로 구성된다. 이 채널을 통한 전송은 모든 참가자들에게 수신되어져야 한다. 어떤 이유에 의해서 수신자가 정당한 시간에 패킷을 수신할 수 없다면, 그룹 관리자와 다시 접속한다. 이것은 또한 반환 채널이 없을 때, out-of-band를 이용하여 수행할 수 있다.

3) 키 관리자(key manager)

수신자에게 TEK를 전달하는 그룹 관리자로부터 재 키잉 요청을 수신하고 복호화한다.

3. 인증 관련

1) 설정 채널(setup channel)

새로운 멤버로부터의 가입 요청은 항상 이 유니캐스트 연결 또는 다른 out-of-band 메커니즘을 통해 수신된다. 이 채널은 새로운 참가자와 그룹 관리자 사이에서 인증을 수행하기 위해서 가입 요청을 부트스트랩 하도록 요구된다.

2) 입회 제어(admission control)

그룹 통신에 가입하기를 원하는 참가자에 대해 접근 제어 목록(ACL: Access Control List)을 통해서 허용과 거부를 검증하는 기능을 수행한다.

3) ACL(access control list)

그룹 접근 제어 목록으로서, 해당 그룹에 대한 입회 제어가 가능하도록 하는 기능을 수행하며, 그룹 초기자에 의해 생성되고 입회제어에서 관리한다.

4) MCert(multicast certificate)

멀티캐스트 인증서는 코어의 입회제어에 의해 생성되어 가입을 요구하는 다른 코어에게 전달된다. 멀티캐스트 인증서의 구성요소는 다음과 같다.

- 버전 번호
- 일련 번호
- 발행자 이름
- 유효 기간
- 멀티캐스트 그룹 식별자
- 멀티캐스트 그룹 초기자 구별 이름
- 그룹 허용/거부 목록
- 송신자 목록
- 전자 서명

Ⅳ. 결 론

멀티캐스트 응용들이 많아지면서, 보안 멀티캐스트 통신은 점차로 중요하게 되었다. 본 논문에서는 현재 멀티캐스트 통신을 위해서 연구가 진행되고 있는 멀티캐스트 라우팅 프로토콜과 현재 사용되고 있는 멀티캐스트 라우팅 프로토콜 중에서 보다 효율적인 보안 체계를 설계할 수 있고 확장성에 있어서도 루트에게 모든 트래픽이 집중되지 않고 중간 라우터에서 인증과 보안키를 교환 할 수 있는 공유 트리를 기반으로 하는 CBT를 이용하여 멀티캐스트 보안 시스템을 설계하였다.

또한 이러한 멀티캐스트 보안 시스템을 설계하기 위하여 현재 멀티캐스트에서 발생 가능한 보안위협에 대한 5가지의 보안 서비스를 분석하였고, 이러한 보안 서비스를 제공하기 위한 보안 시스템의 구성요소를 연구하여 통합적으로 운영할 수 있는 보안 시스템을 제안하였다. 그리고 단일 코어뿐만 아니라 다중 코어를 가진 다중 통신 환경에서도 코어간에 원활하게 그룹정보를 전달할 수 있도록 그룹 인증서를 설계하였다.

참 고 문 헌

[1] 국내문헌

1) 이호영(2007), 효율적으로 확장성을 제공하는 실용적인 IPv6 멀티캐스트 보안 시스템, 건국대 대학원 박사학위 논문.
2) 노종혁, 진승헌(2005), "보안 이동 멀티캐스트를 위한 키 관리 방법", 한국컴퓨터종합학술대회 논문집. 제32권 제2호(I), pp.106-108.
3) 윤미연, 정현철, 원유재(2008), "ITU-T SG17에서의 IPTV 및 멀티캐스트 보안 표준화 동향", 정보보호학회지 제18권 제4호, pp.42-48.
4) 박종열, 문진영, 김정태, 백의현(2007), "ITU-T FG IPTV Security Aspects 표준화 기술 동향", 전자통신동향분석. 제22권 제5호, pp.130-143.
5) 고훈(2004), 이동 IPv6 환경에서 안전한 그룹전송을 위한 인증 방안에 관한 연구, 숭실대 대학원 박사학위 논문.

[2] 외국문헌

1) H. Harney, C. Muckenhirn(2007), "Group Key Management Protocol(GKMP) Specification," Request for Comments 2093, Internet Activities Board.
2) A. Ballardie(2007), "Core Based Tree(CBT) Multicast Routing Architecture," Request for Comments 2201, Internet Activities Board, Sept 2007.
3) T. Ballardie, P. Francis, J. Crowcroft(2003), "Core Based Tree - An Architecture for Scalable Inter Domain Mutlricast Routing," In Proceedingof ACM SIGCOMM, pp 85-95.
4) T. Ballardieand, J. Crowcroft(2005), "Multicast-specific security threats and counter-measure," Proceedings of the Symposium on Network and Distributed System Security.
5) L. Gong, N.Shacham(2004), "Elements of Trusted Multicasting," Technical Report SRI-CSL-94-03, Computer Science Laboratory, SRI International.